# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

## INDICE

# 1 INTRODUCCIÓN.

La información física o electrónica de la notaría es un activo valioso, por tal razón, se debe tener conciencia de la importancia que representa y las consecuencias que pueden traer la pérdida, alteración, acceso no autorizado o mal intencionado a esta. La información de la notaría no se escapa a las amenazas de seguridad que a diario enfrenta, como: desastres naturales, incendio, inundación, sabotaje, vandalismo, robo, posibilidad de daños y pérdidas por causa de códigos maliciosos, ataques de denegación de servicios o simplemente mal uso.

Los datos y la información del Notario deben ser protegidos con estrategias que permitan su administración y control para garantizar la seguridad, autenticidad, confidencialidad, disponibilidad e integridad de la información en su despacho.

La implementación, seguimiento, aplicación y mejora continua de la Política de Seguridad de la Información en la notaría, asegura protección a la información frente a muchas amenazas y contribuye a minimizar riesgos asociados de daño y a garantizar el cumplimiento de las funciones del Notario, sus directivos, funcionarios, usuarios y terceros que tienen relación con los datos y la información en el despacho notarial.

# 2 OBJETIVO.

Establecer y presentar Política de Seguridad de la Información para garantizar la integridad, disponibilidad, actualización, no repudio, confidencialidad y seguridad de la información y del uso del sistema en la oficina del Notario, Esta Política se debe dar a conocer a los directivos, funcionarios, usuarios y terceros que presten sus servicios o tengan relación con los activos de la información de la notaría, para su cabal cumplimiento.

# 3 ALCANCE.

La Política de Seguridad de la Información está dirigida a todas las dependencias, recursos y procesos internos o externos que componen o tienen que ver con los datos o la información de la notaría y debe ser cumplida por sus directivos, funcionarios, usuarios y terceros que tengan relación con la información, asegurando su calidad, protección y

seguridad y generando las medidas preventivas y correctivas necesarias para conseguir el logro del objetivo de este manual de Política de Seguridad de la Información.

# 4 TÉRMINOS Y DEFINICIONES.

**Accesos autorizados:** Autorizaciones concedidas a un usuario para la utilización de los diversos recursos, sin que pueda utilizarlos para fines propios.

**Activo de información:** Todo aquello que se considera importante o que tiene valor para el Notario, ya que puede contener información fundamental. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para el Notario. Se pueden clasificar:

- **Datos:** Son todos aquellos elementos básicos de la información, en cualquier formato, que se generan, recogen, gestionan, transmiten y destruyen en la notaría.

- **Aplicaciones:** Es todo el software que se utiliza para la gestión de la información de la notaría.

- **Personal:** Es todo el personal de la notaría, el personal subcontratado, los clientes, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información del Notario.

- **Servicios:** Son tanto los servicios internos, aquellos que una parte de la notaría suministra a otra, como los externos, aquellos que la notaría suministra a clientes y usuarios.

- **Tecnología:** Son todos los equipos utilizados para gestionar la información y las comunicaciones en la notaría.

**Acuerdo de Confidencialidad:** Documento en los que los funcionarios, usuarios o terceros manifiestan su voluntad de mantener la privacidad de la información de la notaría, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso, en virtud de la labor que desarrollan dentro despacho notarial.

**Amenaza:** Situación que desencadena incidentes en la notaría y que comprometen los activos de información del Notario.

**Autenticación:** Es la confianza o verificación de que un recurso humano u objeto, es realmente quien dice ser.

**Confidencialidad:** Hace referencia a la necesidad de ocultar o mantener secreta determinada información o recursos.

**Control de acceso:** Mecanismo que en función de la identificación y la autenticación que permite conocer los accesos a datos o recursos.

**Directivo:** Persona encargada por el Notario para administrar la notaría o una de sus dependencias. Estas pueden ser: el Notario encargado, el administrador, el jefe de jurídica o el jefe de alguna de las dependencias de la notaría.

**Disponibilidad:** Garantía de poder usar la información cuando es requerida por un sujeto u objeto autorizado.

**Información:** Conjunto organizado de datos procesados, que constituyen un mensaje que cambia de estado de conocimiento del sujeto o sistema que recibe dicho mensaje. Toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que se genere en desarrollo de la actividad de la notaría.

I**nformación pública.** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

**Información pública clasificada.** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en la ley.

**Información confidencial** es la información privada en poder del Estado cuyo acceso público se prohíbe por mandato constitucional o legal en razón de un interés personal jurídicamente protegido. Es decir, la información referente a la intimidad personal y familiar, al honor y propia imagen, así como archivos médicos cuya divulgación constituiría una invasión a la privacidad de la persona. A esta información solo tendrán acceso las personas que son dueñas de ella.

**Integridad:** Fidelidad de la información. Su objetivo es prevenir modificaciones impropias o no autorizadas de la información.

**Medida correctiva:** Acción de tipo reactivo orientada a eliminar la causa de no

conformidad asociada a la implementación y operación aI sistema de gestión de la seguridad de la información con el fin de prevenir su repetición.

**Medida preventiva:** Acción de tipo pro-activo orientada a prevenir potenciales no conformidades asociadas a la implementación y operación del SGSI.

**Medio de procesamiento:** Mecanismo o recurso utilizado para implementar o aplicar técnicas eléctricas, electrónicas o mecánicas para manipular datos e información para el empleo humano o de máquinas.

**No-repudio:** Capacidad de aprobar que un evento o una acción, de manera que este evento o acción no sea negado posteriormente.

**Política de seguridad:** Documento por el cual se establece un compromiso de dirección y enfoque de la notaría. Documento que establece los procesos y procedimientos más relevantes para manejar el riesgo y mejorar la seguridad de la información del despacho notarial.

**Recursos:** Todas aquellas fuentes que consultamos. Fuentes o suministros del cual se produce un beneficio.

**Recursos de la información:** Medios y bienes que permiten adquirir, ampliar o precisar conocimientos con el fin de resolver la necesidad de una organización.

**Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Combinación de la probabilidad de un evento y sus consecuencias.

**Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, además también pueden estar involucradas otras propiedades de la autenticidad, responsabilidad, no repudio, confiabilidad.

**Software malicioso:** Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

**Terceros:** Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos al Notario.

**Vulnerabilidad:** Puntos débiles de aplicaciones, equipos, personal, procesos y mecanismos de control que facilitan la concreción de una amenaza. Potencial o posibilidad de que se materialice una amenaza.

# 5 POLÍTICA DE SEGURIDAD.

La implementación, mantenimiento, control, divulgación y mejoramiento continuo de la Política de Seguridad de la Información en la notaría garantiza la seguridad, confidencialidad, integridad y disponibilidad de los activos de la información y permite establecer mecanismos y procedimientos para asegurar el eficiente cumplimiento de las funciones del Notario y la labor de sus directivos, funcionarios, usuarios y terceros, minimizando los riesgos y amenazas a los datos y a la información en sus despachos.

## *5.1 REQUISITOS LEGALES Y/O REGLAMENTARIOS.*

El Notario debe respetar y velar por el cabal cumplimiento de los requisitos y las normas legales aplicables y vigentes de acuerdo a la constitución y a la ley por parte de sus directivos, funcionarios, usuarios y terceros que tienen relación con la seguridad de la información en la notaría.

### 5.1.1 MARCO LEGAL

- Constitución Política de Colombia 1991.
- Código Penal Colombiano - Decreto 599 de 2000
- Decreto 960 de 1970- Estatuto del Notariado.
- Ley 906 de 2004, Código de Procedimiento Penal.
- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor.
- Ley 594 de 2000 - Ley General de Archivos.
- Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 2000 y ley 1437 de 2011.
- Ley 527 de 1999, por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 1266 de 2008 o Ley del Habeas • Data que regula el manejo de la información contenida en base de datos personales.
- Ley 1581 de 2012 para la Protección de Datos Personales.
- Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012.
- Ley 1273 de 2009, Delitos Informáticos protección de la información y los datos.
- Ley 29 de 1973.
- Ley 1712 de 2014
- Decreto 2668 de 1988.

- Decreto 1157 de 1989.
- Decreto 1712 de 1989.
- Decreto 2148 de 1989.

## *5.2 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.*

El objetivo de la Política de Seguridad de la Información es asegurar una apropiada protección a la información de la notaría, estableciendo reglas con las que se deben operar los recursos y procesos de la información para minimizar riesgos y garantizar la seguridad, confidencialidad, integridad y disponibilidad de los activos del Notario.
Esta Política debe ser conocida y aplicada por directivos, administradores, funcionarios, usuarios, terceros y en general por todos los usuarios de la información según las funciones que realicen y que tengan relación con la notaría. La no aplicación de la Política de Seguridad de la información implica sanciones, según el caso que se presente.

El Comité de Seguridad de la Información y los funcionarios de la notaría, con el fin de minimizar y eliminar los riesgos a que se expone la información en sus dependencias, deben identificar dichos riesgos, ya que la información de la notaría puede ser modificada, copiada, divulgada o destruida.

### 5.2.1 RESPONSABLES DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

El Notario debe garantizar y apoyar el proceso e implementación, mantenimiento y actualización de la Política de Seguridad de la información en la notaría, por tal razón debe crear un Comité de Seguridad de la Información, responsable de determinar, establecer, controlar, mantener, mejorar y asegurar la Política, para el correcto uso de los activos de información en su despacho. Este Comité debe estar conformado por el Notario, un Directivo y un Coordinador del Comité que será nombrado por el Notario.

El Notario y su Comité de Seguridad de la Información son responsables de la autorización de las modificaciones, revisiones y actualizaciones que se hagan a la Política de Seguridad de la Información.

### 5.2.2 DOCUMENTAR LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

El Comité de Seguridad de la Información es el responsable de crear el documento o manual de Política de Seguridad de Información, que debe ser aprobado por el Notario, publicado y comunicado a todos los directivos, funcionarios, usuarios y terceros que tengan relación con los datos y la información, de acuerdo a su correspondencia y velar por su obligatorio cumplimiento.

Se debe garantizar que la notaría cuente con los documentos rigurosamente necesarios dependiendo el perfil de actuación de cada funcionario y la dependencia en que se desempeña. Los documentos deben ser manejados y controlados asegurando su confidencialidad, integridad y disponibilidad.

### 5.2.3 REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

La Política de Seguridad de la Información en la notaría debe ser revisada, auditada y actualizada anualmente por el Comité de Seguridad de la Información para garantizar su idoneidad, eficiencia y efectividad. Este Comité debe verificar que se cumpla.

# 6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

El Notario y su Comité de Seguridad de la Información deben garantizar y apoyar el proceso de implementación, operación, control, mantenimiento, revisión y mejora de la Seguridad de la Información en la notaría.

Este Comité tiene que revisar y actualizar anualmente Política de Seguridad de la Información, después de presentada al Notario y su correspondiente aprobación. Dicha actualización debe seguir las directrices y procedimientos estipulados en esta Política y en los estándares y normas legales vigentes. También debe asegurar el debido proceso de la información y la protección adecuada de la información con respecto a la organización de la notaría.

El Comité de Seguridad de la Información debe definir las actividades y los resultados que espera obtener de los directivos, funcionarios, usuarios y terceros en cumplimiento de cada labor y que tengan relación con los datos y la información de la notaría.

## *6.1 ORGANIZACIÓN INTERNA.*

El Comité de Seguridad de la Información se encarga de manejar la seguridad de la información dentro de la notaría.

### 6.1.1 COMPROMISO DEL NOTARIO Y LOS DIRECTIVOS CON LA SEGURIDAD DE LA INFORMACIÓN.

El Notario y sus directivas deben apoyar activamente la seguridad de la información y al Comité de Seguridad de la Información en la notaría, exponiendo claramente las instrucciones y asignando responsabilidades que contribuyan al buen manejo de la seguridad de la información en su despacho.

### 6.1.2 ASIGNACIÓN DE RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN.

Toda información debe ser apropiadamente identificada, clasificada y documentada, para así definir los responsables, responsabilidades, custodia y permisos de acceso a la información de la notaría. La información debe clasificarse de acuerdo a las guías de clasificación establecidas por el Comité de Seguridad de la Información y por las normas y estándares legales vigentes para el funcionamiento de la notaría.

### 6.1.3 PROCESO DE AUTORIZACIÓN PARA LOS MEDIOS DE PROCESAMIENTO DE LA INFORMACIÓN.

El Comité de Seguridad de la Información de la notaría debe definir e implementar un protocolo de autorizaciones para el uso de los medios de procesamiento de la información y, en ningún caso, está permitido a funcionarios, usuarios o terceros el acceso a estos, sin previa autorización del directivo de la notaría o del directivo de la respectiva dependencia.

### 6.1.4 ACUERDOS DE CONFIDENCIALIDAD.

Todo directivo, funcionario, usuario o tercero que tenga acceso a la información de la notaría deberá garantizar la completa confidencialidad mediante estipulaciones contenidas en los respectivos contratos y/o compromisos de confidencialidad.

## *6.2 INTERCAMBIO DE INFORMACIÓN CON ORGANIZACIONES EXTERNAS.*

El Comité de Seguridad de la Información de la notaría debe mantener la seguridad y los servicios de procesamiento de información, a los cuales acceden usuarios, terceros, empresas o entidades externas; o los que son comunicados, procesados o dirigidos por estas. El Comité debe seguir los estándares de gestión de calidad y seguridad de la información, identificando los riesgos que se pueden presentar con el intercambio de información con personas u organizaciones externas y estableciendo controles de seguridad de acuerdo a los criterios establecidos por el Notario y por el Comité.

Las peticiones de intercambio de información por parte de entes externos deben ser aprobadas por el Notario y el Comité de Seguridad de la Información y dirigidas de acuerdo a la Política de Seguridad establecidas en la notaría, con la continua y estricta supervisión del Comité.

El Comité de Seguridad de la Información de la notaría debe velar para que el personal provisto por terceras partes tenga acceso únicamente a la información necesaria para el desarrollo de sus labores y para que la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

La información sensible debe ser encriptada de forma que solo las personas autorizadas puedan acceder a ella.

Cualquier información intercambiada por medios electrónicos (USB, correo electrónico, descarga) debe ser analizada con antivirus previo contacto con el sistema de información.

### 6.2.1 IDENTIFICACIÓN DE LOS RIESGOS Y TRATAMIENTO DE LA SEGURIDAD.

El Comité de Seguridad de la Información de la notaría debe contar con un documento de identificación y valoración de riesgos de la información. Se debe evitar desarrollar procesos que asocien riesgos altos no mitigados en los despachos del Notario.

El Comité de Seguridad de la Información del círculo notarial debe evaluar periódicamente las amenazas y vulnerabilidades hacia la información o instalaciones de procesamiento de esta, la ocurrencia, su impacto y el desarrollo de estrategias para manejarlas y mitigarlas.

### 6.2.2 TRATAMIENTO DE LA SEGURIDAD PARA USUARIOS.

Los usuarios de la notaría solo pueden acceder a los datos o recursos de la información catalogados como públicos y a los permitidos conforme a la constitución y las leyes. El Comité de Seguridad de la Información de la notaría es el responsable de controlar y vigilar el uso adecuado de la información y los recursos de la notaría por parte de los usuarios.

### 6.2.3 TRATAMIENTO DE LA SEGURIDAD EN CONTRATOS CON TERCERAS PERSONAS.

De acuerdo a la información intercambiada y a la clasificación de la misma, los contratos entre terceras personas y el Notario, deben contener cláusulas de confidencialidad y compromisos de servicio que permitan cumplir con los objetivos y la Política de Seguridad de la Información de la notaría.

## 7 GESTIÓN DE ACTIVOS.

El Comité de Seguridad de la Información debe tener como objetivo la protección adecuada de los activos de la información del Notario.

## *7.1 RESPONSABILIDAD POR LOS ACTIVOS.*

El Comité de Seguridad de la Información es el responsable de los activos de la información del Notario y de practicar periódicamente auditorias sobre los procesos, actividades y sistemas vinculados con la gestión de activos de la información del Notario. También es el responsable del cumplimiento de las medidas y especificaciones establecidas en esta Política de Seguridad de la Información.

### 7.1.1 INVENTARIOS DE ACTIVOS.

El Comité de Seguridad de la Información debe determinar y mantener un inventario actualizado, de todos los activos de la información del Notario, los cuales deben estar claramente identificados de acuerdo a cada una de las dependencias de la notaría.

### 7.1.2 PROPIEDAD DE LOS ACTIVOS.

El Notario es el propietario de todos los activos de la información y el Comité de Seguridad de la Información de la notaría es el responsable y administrador de ellos.

### 7.1.3 USO ACEPTABLE DE LOS ACTIVOS.

El Comité de Seguridad de la Información debe identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la misma, logrando mantener una adecuada protección de los activos de la información y aplicación de la Política de Seguridad de la Información por parte del Notario, sus directivos, funcionarios, usuarios y terceros que tengan relación con los activos de la información para el cumplimiento de los propósitos generales de la notaría. El Comité de Seguridad de la Información de la notaría, para el uso adecuado de los activos de la información, debe tener en cuenta y hacer cumplir las siguientes directrices:

- Los activos de la información pertenecen al Notario y su uso debe ser única y exclusivamente para el cumplimiento de los propósitos de la notaría.
- Los funcionarios y terceros deben usar únicamente los activos de la información

autorizados por el Comité de Seguridad de la Información.

- La posibilidad de acceso a los activos de la información de la notaría, por parte de directivos, funcionarios, usuarios o terceros, no implica el permiso de uso, por consiguiente no debe leer, modificar copiar, transmitir o borrar información sin la debida autorización.

- Cuando los funcionarios de la notaría impriman, saquen copias, escaneen o manden faxes, deben verificar los lugares adyacentes a las herramientas u equipos utilizados, para asegurar que no se queden documentos relacionados y así evitar el acceso o divulgación no autorizada a los activos de la información del Notario.

- Los directivos, funcionarios y terceros, al momento de ausentarse de sus escritorios o puestos de trabajo, deben asegurarse de cerrar la sesión de los aplicativos o sistemas de información y verificar que sus escritorios se encuentren libres de documentos y medios de almacenamiento utilizados para el desempeño de sus funciones en la notaría.

- A no ser que exista una aprobación por escrito, los directivos, funcionarios o terceros no deben explotar las vulnerabilidades o deficiencias de seguridad de los medios (software, páginas web, servidores, archivadores) que almacenan o faciliten la información de la notaría.

- La información que se encuentre bajo custodia en la notaría debe ser protegida bajo controles de acceso físico y buenas condiciones de almacenamiento y resguardo.

- Está prohibida la ingestión de bebidas u otro tipo de alimentos sobre o en las proximidades de cualquiera de los documentos, archivadores, computares, aparatos electrónicos o demás activos de la información con que cuenta el Notario en sus despachos, así como el manejo de sustancias o elementos que puedan ocasionar daños a los mismos.

- En caso de que directivos, funcionarios o terceros encuentren vulnerabilidades o riesgos que comprometan la seguridad de la información de la notaría, estas deben ser reportadas de inmediato al Comité de Seguridad de la Información.

- Los usuarios de la notaría solo pueden acceder a los datos o recursos de la información catalogados como públicos y a los permitidos conforme a la constitución y las leyes.

- El Comité de Seguridad de la Información es el encargado de suministrar a cada

funcionario los equipos, programas y recursos informáticos; los datos e información creados, almacenados y recibidos, serán propiedad del Notario.

- El Comité de Seguridad de la Información de la notaría es el encargado de realizar las copias de seguridad o backup de la información de la notaría, de manera periódica y frecuente, la cual debe ser almacenada en sitios apropiados para garantizar la seguridad de la misma y que se pueda recuperar en caso de desastres o incidentes con los equipos de procesamiento.

- Los directivos, funcionarios y terceros solo podrán realizar backup de la información de la notaría conforme lo establezca el Comité de Seguridad de la Información de la notaría. Cualquier otro tipo de copia o backup debe ser con autorización del Comité y de acuerdo a la clasificación de la información.

- La modificación, copia, sustracción, daño intencional o utilización para fines distintos a los propósitos de la notaría, son sancionadas de acuerdo con lo establecido en la Política de Seguridad de Información de la notaría y en las normas y legislación vigentes.

- El Comité de Seguridad de la Información de la notaría debe inventariar, revisar y auditar los activos de la información utilizados en cada dependencia de la notaría.

- La descarga, instalación o uso de aplicativos o programas informáticos no autorizados por el Comité de Seguridad de la Información de la notaría son sancionadas conforme a las Política de Seguridad de la Información del Notario.

- El Comité de Seguridad de la Información de la notaría es la encargada de tener bajo custodia los medios magnéticos y electrónicos, como: disquetes, CDs, manuales, licencias de uso, claves para descargar el software de fabricantes de sus páginas web o sitios en internet, los passwords de administración de los equipos informáticos, sistemas de información o aplicativos, etc.

- Los activos de la información del Notario no pueden ser utilizados, sin previa autorización escrita del Comité de Seguridad de la Información de la notaría, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o para otro uso que no esté autorizado.

- Los directivos, funcionarios, usuarios y terceros de la notaría que intenten actos que atenten contra el buen uso de los activos de la información del Notario, como: envió

de correo electrónico masivo con fines diferentes a los propósitos de la notaría y práctica de juegos en línea, deben ser sancionados conforme a lo estipulado en la Política de Seguridad de la Información de la notaría.

- El Comité de Seguridad de la Información de la notaría es el encargado de la aprobación y autorización de: Instalación de software en equipos de la notaría; descarga de software de Internet u otro servicio en línea en cualquier equipo de la notaría; modificación, revisión, transformación o adaptación de software de propiedad del Notario; Copiar o distribuir software de propiedad del Notario.

- Los directivos, funcionarios, usuarios y terceros son responsables de todas las transacciones o actuaciones realizadas con su cuenta de usuario.

- Los directivos, funcionarios, usuarios y terceros no pueden acceder a la red o a otros servicios utilizando una cuenta de usuario o clave de otro usuario de la notaría.

- Las peticiones de intercambio de información por parte de entes externos deben ser aprobadas por el Notario y el Comité de Seguridad de la Información y dirigidas de acuerdo a la Política de Seguridad establecida en la notaría, con la continua y estricta supervisión del Comité.

- El Comité de Seguridad de la Información de la notaría es el responsable de: asegurar el acceso a los activos de la información del Notario, así como los accesos a Internet, a redes sociales o de terceros; prevenir el acceso no autorizado de usuarios o terceros; controlar la introducción o propagación de programas destructivos o virus

- El Comité de Seguridad de la Información de la notaría debe revisar todos los materiales, archivos o descargas de redes externas para detectar programas destructivos y virus.

- El Comité de Seguridad de la Información de la notaría es el encargado de aprobar, autorizar y controlar los cambios en la infraestructura informática de la notaría.

## *7.2 CLASIFICACIÓN DE LA INFORMACIÓN.*

El Comité de Seguridad de la Información de la notaría debe asegurar que los activos de información del Notario reciban una adecuada clasificación, etiquetado, manejo y protección, de acuerdo a la Política de Seguridad de la Información de la notaría y de los

estándares y normas legales vigentes, garantizando la integridad, confidencialidad, disponibilidad y seguridad de la información.

El Notario puede almacenar la información en medios de la información, como: Servidores, protocolo, bases de datos, medios magnéticos y electrónicos, archivadores con carpetas que contienen actas, documentos, contratos, etc.

### 7.2.1 LINEAMIENTOS DE CLASIFICACIÓN.

Los directivos y funcionarios deben identificar y valorar los activos de información de la notaría, de los cuales son responsables, con la finalidad de seguir los lineamientos de clasificación establecidos por el Comité de Seguridad de la Información de la notaría, conforme a la Política de Seguridad de la Información y de los estándares y normas legales vigentes y para garantizar la integridad, confidencialidad, disponibilidad y seguridad de la información.

Conforme a la normatividad legal vigente la información de la notaría se clasifica en:

- Información Pública
- Información Pública Clasificada
- Información Confidencial

El Comité de Seguridad de la Información para asegurar los activos del Notario, también debe identificar la información confidencial y clasificar la información que se puede divulgar, así: Según limitaciones de uso y según el valor de la información. Esto con el fin de que pueda dar a conocer esta clasificación a los directivos, funcionarios, terceros y usuarios y se garanticen buenas prácticas para proteger la información, su integridad, confidencialidad y disponibilidad.

Información de acuerdo a limitaciones de uso:

- Información de uso general. Se puede compartir fuera de la notaría, como dentro de la notaría.
- Información restrictiva. Es información sensible que puede perjudicar a una persona natural o jurídica.
- Información confidencial. Su uso no autorizado puede ocasionar grandes perjuicios a los intereses económicos y comerciales de una persona natural o jurídica.

Según el valor de la información:

- Información clave. Su pérdida perjudicaría la continuidad de un proyecto o proceso del Notario.
- Información no vital. Su no disponibilidad no afecta la actividad de la Notaría.

# 8 SEGURIDAD DE LOS RECURSOS HUMANOS.

El Comité de Seguridad de la Información de la notaría debe garantizar que los directivos, funcionarios y terceros que tienen relación con los activos de información de la notaría acaten con responsabilidad la Política de Seguridad de la Información y hagan un adecuado uso de los activos de información del Notario, de acuerdo a dependencia, tarea que desempeñan y a la situación contractual con la notaría.

El Comité de Seguridad de la Información de la notaría debe definir un perfil para todo el personal que tiene relación con los activos de información del Notario y debe conservar un directorio completo y actualizado de tales perfiles.

## *8.1 ROLES, RESPONSABILIDADESY FUNCIONES.*

Los directivos, funcionarios y terceros que tienen relación con los activos del Notario, deben asegurar y entender sus responsabilidades en relación con la Política para la Seguridad de la Información del Notario y actuar de manera consecuente frente a ella, con el objetivo de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado o mal intencionado de los activos de la información del Notario.

El Comité de Seguridad de la Información de la notaría debe elaborar, mantener, actualizar, mejorar y difundir el manual de Responsabilidades Personales para la seguridad de la información en el despacho del Notario.

El Notario es el encargado de contratar y definir los perfiles para el personal que tiene que ver con los activos de la información.

- El Comité de Seguridad de la Información de la notaría es responsable de revisar y proponer el texto de la Política de Seguridad de la Información de la notaría y asignar las funciones generales que deben cumplir los directivos, el coordinador del Comité,

los funcionarios y terceros que tienen relación con la información del despacho notarial.

- El Coordinador del Comité de Seguridad de la Información de la notaría es el responsable de coordinar las acciones del Comité y de impulsar la implementación y cumplimiento de la Política de Seguridad de la Información por parte de los directivos, funcionarios, terceros y usuarios del despacho notarial.

- Todos los funcionarios de la notaría son responsables de proteger la información que está contenida en documentos, formatos, listados, equipos, sistemas etc., derivado de sus funciones y que son el resultado de los procesos informáticos.

- Cada dependencia de la notaría debe mantener depurada la información de las carpetas virtuales para la optimización del uso de los recursos de almacenamiento y debe velar por la seguridad de los medios de la información de los que son responsables.

- Los terceros son responsables de asegurar y mantener la Política de seguridad de la información de los activos de la información que suministran al Notario.

- Los directivos son responsables de definir los permisos de acceso a la información que autoriza a los funcionarios de acuerdo a sus funciones y competencia para que se mantenga y asegure la integridad., confidencialidad y disponibilidad de la información en la notaría.

- El administrador o directivo responsable de la notaría debe cumplir la función de notificar al personal que se vincule contractualmente con el Notario, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la información de todos los estándares, procesos, prácticas y guías que surjan del sistema de la Seguridad de la información. También es el responsable de informar los cambios que en ella se produzcan y suscribir compromisos de confidencialidad.

## *8.2 PROCESO DISCIPLINARIO.*

Sin perjuicio de las demás disposiciones legales aplicables que la conducta pueda ocasionar, es necesaria la clasificación de las violaciones a la Políticas de Seguridad de la notaría, con el fin de aplicar medidas correctivas conforme a la clasificación definida y mitigar la afectación a la seguridad de los activos de la información del Notario.

Se considerarán entre las medidas correctivas: llamados de atención y acciones administrativas de orden disciplinario o penal, de acuerdo a las circunstancias que así lo ameriten.

El Notario es el encargado de imponer los procesos y medidas disciplinarias para los casos que se presenten por usos indebidos o malintencionados de los activos de la información y que violan la Política de Seguridad de la Información de la notaría.

## *8.3 TERMINACIÓN O CAMBIO DE FUNCIÓN Y ELIMINACIÓN DE DERECHOS DE ACCESO.*

A la terminación del contrato o cambio de labor de los directivos, funcionarios o terceros, deben, inmediatamente, ser revocados los mecanismos de autenticación y controles de acceso y devuelto todos los activos de la información del Notario, otorgados con ocasión del contrato o acuerdo.

## *8.4 DEVOLUCIÓN DE ACTIVOS.*

A la terminación del contrato de directivos, funcionarios o terceros deben ser devueltos, al Comité de Seguridad de la Información, todos los activos de la información del Notario, que le fueron puestos a disposición con ocasión del desempeño de la labor.

# 9 SEGURIDAD FÍSICA Y AMBIENTAL.

El objetivo de la Política de Seguridad de la Información física y ambiental es impedir acceso no autorizado a las áreas donde se encuentran los activos de información, evitando así posibles daños o perjuicios en la prestación de los servicios.

## *9.1 ÁREAS SEGURAS.*

Los lugares físicos donde se encuentran los medios que contienen servidores, almacenes principales de datos, equipos, cableado estructurado, conexiones de red, documentos o

cualquier activo de información de uso reservado del Notario deben estar en áreas seguras y con un sistema de seguridad que no permita el acceso de terceros a dichas áreas.

### 9.1.1 CONTROLES DE ENTRADA FÍSICOS.

El Comité de Seguridad de la Información de la notaría debe controlar y restringir el acceso de personas no autorizadas a las áreas seguras. Se debe dejar registro, de fecha y hora, de los terceros o usuarios autorizados que ingresan a las áreas seguras de la notaría.

### 9.1.2 PERÍMETROS DE SEGURIDAD FÍSICA.

La notaría debe contar con barreras y puertas de seguridad física para evitar el ingreso a las áreas que contienen documentos, información o medios de procesamiento de la información.

### 9.1.3 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES.

En la notaría se debe aplicar protección contra incendios, inundación, explosión, robo u otras catástrofes que puedan afectar, modificar o acabar con los activos de la información del Notario.

No se deben almacenar materiales peligrosos o combustibles que puedan afectar los activos de la información del Notario.

## *9.2 SEGURIDAD DEL EQUIPO.*

Todo equipo debe ser revisado, registrado y aprobado por el Comité de Seguridad de la Información de la notaría cumpliendo con todos los requisitos y controles establecidos. Únicamente podrán realizar las tareas para las que fueron autorizados.

Los servidores y equipos que contengan información de la notaría, deben estar ubicados en áreas seguras con controles de acceso, seguridad física y ambiental y respaldados con UPS.

### 9.2.1 MANTENIMIENTO DE EQUIPO.

Los equipos de la notaría deben recibir mantenimiento y soporte de hardware y software constante con el fin de asegurar la disponibilidad de los servicios.

Los puestos de trabajo deben tener bien asegurados los equipos y deben ser operados únicamente por los directivos, funcionarios o terceros autorizados por el Comité de Seguridad de la Información de la notaría.

El Comité de Seguridad de la Información debe informar de la Política de Seguridad de la Información del Notario a los directivos, funcionarios o terceros autorizados para el uso responsable de los equipos y recursos de la información.

Las copias de seguridad deben ser conservadas de acuerdo a la Política de Seguridad de la Información de la notaría y a los estándares vigentes.

### *9.2.2 SEGURIDAD DEL EQUIPO FUERA DEL LOCAL.*

El Comité de Seguridad de la Información debe implementar Política de Seguridad para proteger los medios de la información que se requieran sacar de las instalaciones de la notaría.

Las Política de Seguridad de la Información implementada en los equipos que se requieren sacar del despacho notarial deben tener en cuenta los riesgos a que se expone y la forma de mitigarlos.

### 9.2.3 ELIMINACIÓN SEGURA O RE-USO DEL EQUIPO.

El Comité de Seguridad de la Información es el encargado de determinar re-usar o eliminar equipos o medios de información de la notaría.

Los equipos o medios de información de la notaría que vayan a ser re-usados o eliminados deben surtir un proceso de borrado seguro y posteriormente serán re-usados, eliminados o destruidos de forma adecuada. Se debe realizar la destrucción de información cuando se ha cumplido su ciclo de almacenamiento.

# 10 GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES.

El Comité de Seguridad de la Información de la notaría debe asegurar la operación correcta de los medios de procesamiento de la información.

## *10.1 PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES.*

Un procedimiento describe de forma más detallada de lo que se hace en las actividades de un proceso de la notaría, en él se especifica cómo se deben desarrollar las actividades, cuáles son los recursos, el método y el objetivo que se pretende lograr o el valor agregado que genera y caracteriza los procesos en la notaría.

El Notario y su Comité de Seguridad de la Información elaboran y aprueban la Política de Seguridad de la Información, de acuerdo con las necesidades y el compromiso de diseño e implementación de estrategias eficientes que garanticen la correcta y segura operación de los medios de procesamiento, recursos y activos de la información en la notaría.

El Comité de Seguridad de la Información debe elaborar los instructivos para detallar aún más las tareas y acciones puntuales que se deben desarrollar dentro de un procedimiento, como son los instructivos de trabajo y de operación; los primeros para la ejecución de la tarea por la persona y los segundos para la manipulación o la operación de un equipo y que tengan que ver con los datos y la información de la notaría.

### 10.1.1 PROCEDIMIENTO DE OPERACIÓN DOCUMENTADOS.

El Comité de Seguridad de la Información se encargará de elaborar y mantener actualizados los manuales de los procedimientos de operación implementados en la notaría y los divulgará a los directivos, funcionarios, usuarios y terceros que tengan relación con los datos y la información del despacho notarial.

### 10.1.2 GESTIÓN DE CAMBIO.

El Comité de Seguridad de la Información será el encargado de aprobar y controlar los cambios en los medios y en los sistemas de procesamiento de la información de la notaría.

### 10.1.3 SEGREGACIÓN DE DEBERES.

El Comité de Seguridad de la Información debe definir los roles y responsabilidades, así como la persona encargada y autorizada para el control de los medios y sistemas, para evitar del mal uso o de las modificaciones no autorizadas o mal intencionadas los activos de la notaría.

## *10.2 GESTIÓN DE LA ENTREGA DEL SERVICIO DE TERCEROS.*

El Comité de Seguridad de la Información de la notaría debe implementar y mantener una apropiada seguridad de los activos de la información del Notario y de los productos y servicios de información contratados con consultores, contratistas o proveedores.

### 10.2.1 ENTREGA DEL SERVICIO.

El Comité de Seguridad de la Información de la notaría debe asegurar que se implementen, operen y mantengan los controles de seguridad, definiciones de servicio y de entrega, al momento de la contratación de servicios y productos de información con terceros.

### 10.2.2 MONITOREO Y REVISIÓN DE LOS SERVICIOS DE TERCEROS.

Los servicios, reportes y servicios suministrados por terceros al Notario, deben ser monitoreados, revisados y auditados regularmente de conformidad a lo establecido por el Comité de Seguridad de la Información de la notaría y conforme a la Política de Seguridad de la Información y de las normas legales vigentes.

### 10.2.3 MANEJO DE LOS CAMBIOS EN LOS SERVICIOS DE TERCEROS.

El Comité de Seguridad de la Información de la notaría debe estar atento a los cambios en el suministro de los servicios informáticos. Debe mantener y mejorar la Política de Seguridad de la Información, los procedimientos y controles de seguridad teniendo en

cuenta los procesos comerciales, el grado crítico y reevaluando de riesgos.

## *10.3 PROTECCIÓN CONTRA SOFTWARE MALICIOSO.*

El Comité de Seguridad de la Información de la notaría debe elaborar, mantener y controlar Política de Seguridad de la Información, procedimientos, estándares y normas para proteger los sistemas informáticos, teniendo en un enfoque que involucre controles físicos, humanos y técnicos que garanticen la mitigación de riesgos asociados a software malicioso y técnicas de hacking.

Se debe monitorear regularmente el software instalado, como también analizar el equipo con herramientas que aseguren la no presencia de software malicioso, que comprometan la seguridad de la información.

El Comité de Seguridad de la Información debe garantizar que las estaciones de trabajo se encuentren protegidas con antivirus con capacidad de actualización automática.

## *10.4 RESPALDO O BACK-UP.*

Toda información que sea fundamental para el funcionamiento de la notaría se debe respaldar por una copia de seguridad, tomadas conforme lo disponga el Comité de Seguridad de la Información y deber incluir lo referente al almacenamiento de dichas copias.

El Comité de Seguridad de la Información de la notaría es el encargado de elaborar las directrices para el manejo, control, administración y protección de las copias de seguridad de la información de la notaría. Los funcionarios deben entregar periódicamente los back-up correspondientes a la información de sus dependencias conforme lo establezca dicho Comité.

## *10.5 GESTIÓN DE SEGURIDAD EN LA RED.*

El Comité de Seguridad de la Información de la notaría es el encargado de definir autorizar y definir las condiciones y los perfiles de acceso a la red.

Está prohibido el uso de los recursos o acceso a internet para tareas diferentes a las asignadas y la instalación de software o hardware, sin previa autorización del Comité de Seguridad de la Información de la notaría.

Se debe monitorear regularmente el software instalado, como también analizar el equipo con herramientas que aseguren la no presencia de software malicioso, que comprometan la seguridad de la información.

Se deben actualizar y parchear todo software (sistemas operativos, servidor de base de datos, servidor web) para prevenir el acceso a estos por medio de cualquier vulnerabilidad conocida.

## *10.6 GESTIÓN DE MEDIOS.*

Ningún directivo, funcionario, usuario o tercero puede divulgar, modificar, eliminar o destruir los activos de la información del Notario sin autorización expresa de él o del Comité de Seguridad de la Información de la notaría.

El Comité de Seguridad de la Información de la notaría debe establecer los procedimientos y el control de la eliminación de los medios de una manera segura cuando ya no los requiera el Notario, lo mismo que, el procedimiento para almacenar y proteger la información de la notaría de divulgación no autorizada o mal uso.

El acceso a la documentación de la notaría debe ser conforme a la Política de Seguridad de la Información, a los estándares y disposiciones legales vigente.

## *10.7 INTERCAMBIO DE INFORMACIÓN.*

Las peticiones de información por parte de entes externos de control deben ser aprobadas por el Notario o por el Comité de Seguridad de la Información de la notaría y deben ser dirigidas por estos ante los responsables de la custodia.

La información sensible debe ser encriptada de forma que solo las personas autorizadas puedan acceder a ella.

Cualquier información intercambiada por medios electrónicos (USB, correo electrónico, descarga) debe ser analizada con antivirus previo contacto con el sistema de información.

## *10.8 SERVICIOS DE COMERCIO ELECTRÓNICO.*

El Comité de Seguridad de la Información de la notaría es el encargado de autorizar, controlar y auditar el uso responsable de internet y de los servicios de correo electrónico, conforme a la Política de Seguridad de la Información y las normas legales y vigentes.

## *10.9 MONITOREO.*

El Comité de Seguridad de la Información debe establecer mecanismos y procedimientos que le permitan:

- Producir registros de actividades de auditoría y mantenerlos durante un periodo estipulado para contribuir con investigaciones futuras y monitoreo de control de acceso.
- Monitorear el uso de los medios de procesamiento de la información.
- Proteger los medios de registro y la información del registro contra alteraciones y acceso no autorizado.
- Registrar, analizar y corregir las fallas.

# 11. CONTROL DE ACCESO.

El Comité de Seguridad de la Información de la notaría debe definir la Política del control de acceso para los usuarios, sistemas de seguridad, sistemas de información, sistema de redes y otros.

Se proveerán mecanismos de autenticación y control de acceso con el fin de salvaguardar los activos de la información del Notario y para que directivos y funcionarios hagan uso responsable de la información a la cual se les autoriza el acceso.

Los directivos y funcionarios son responsables de toda actividad que derive del uso de su usuario o contraseña o mecanismo de autenticación, por ende no deben ser divulgados o cedidos a otros, cumpliendo con las Política de Seguridad de la Información del Notario, para evitar que esta sea revelada o robado.

Los funcionarios no deben permitir que otros usuarios realicen labores bajo sus mecanismos de autenticación. De igual forma, no se deben realizar actividades bajo las de alguien más.

## *11.1 GESTIÓN DE ACCESO DEL USUARIO.*

La notaría bajo la dirección del Comité de Seguridad de la información, deberá mediante un proceso formal realizar la inscripción y des-inscripción de los accesos de los usuarios a los sistemas de información.

Los funcionarios del área de la información y sistemas harán parte del Comité de Seguridad de la Información de la notaría y serán los encargados de controlar los privilegios especiales de los usuarios en sus estaciones de trabajo.

El Comité de Seguridad de la Información de la notaría es encargado de controlar y auditar que los usuarios cumplan la Política de Seguridad de la Información, respecto del acceso del usuario.

## *11.2 RESPONSABILIDADES DEL USUARIO.*

Está prohibido el uso de los recursos o acceso a internet para tareas diferentes a las asignadas.

La responsabilidad de cada usuario es proteger los activos de la información del Notario, que se encuentra en medio físico y magnético, los cuales son producto de los procesos informáticos realizados en la notaría.

## *11.3 CONTROL DE ACCESO A LA RED*

Se debe asegurar que las redes inalámbricas de la organización cuenten con métodos de autenticación que evite accesos no autorizados.

Se tienen que verificar periódicamente los controles de acceso, mecanismo de autenticación y privilegios de funcionarios y usuarios provistos por terceras partes, con el fin de revisar que dichos usuarios tengan únicamente el acceso permitido a aquellos recursos y servicios para los que fueron autorizados.

Las redes de datos, lugares de almacenamiento, y demás recursos de la notaría deben ser debidamente protegidas contra accesos no autorizados a través de mecanismos de autenticación, o control de acceso.

Es obligatorio contar con el formato de creación de mecanismos de autenticación

debidamente autorizado y Acuerdo de Confidencialidad firmado previamente.

Los equipos de cómputo de usuario final que se conecten o deseen conectar a las redes de datos de las dependencias del Notario, deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

Todas las redes con salida a redes públicas deben ser aseguradas con los mecanismos de seguridad pertinentes (Firewalls, mecanismos de autenticación y protocolos de comunicación seguros).

El Notario establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos físicos, tecnológicos y los sistemas de información.

## *11.4 CONTROL DE ACCESO AL SISTEMA OPERATIVO*

Los Sistemas Operativos en todas las estaciones de trabajo deben estar protegidos mediante un usuario y una contraseña la cual debe ser cambiada cada 6 meses.

## *11.5 CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN*

Queda prohibida la instalación de software o hardware sin la debida autorización del Comité de Seguridad de la Información o sin la licencia pertinente.

Se debe monitorear regularmente el software instalado, como también analizar el equipo con herramientas que aseguren la no presencia de software malicioso, que comprometan la seguridad de la información.

Se deben actualizar parchear todo software (sistemas operativos, servidor de base de datos, servidor web) para prevenir el acceso a estos por medio cualquier vulnerabilidad conocida.

Las contraseñas deben ser mayor a 8 caracteres, hacer combinaciones entre minúsculas y mayúsculas, números y caracteres espaciales como “& @ # -“

En las contraseñas no se deben usar datos de usuario que sean fácilmente deducibles ejemplo, fechas de nacimiento, nombres de personas cercanas o cualquier dato que

guarde relación con el usuario u oficina del Notario.

Hay que evitar utilizar secuencias básicas de teclado (por ejemplo: ”qwerty”, “asdf” o las típicas en numeración: “1234” ó “98765”)

No repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).

No se deben digitar las contraseñas en presencia de personas que puedan observarlas.

Abstenerse de utilizar los mecanismos de autenticación en equipos que no pertenezcan a la oficina donde el Notario ejerce sus funciones o que no estén autorizados para realizar las tareas encomendadas.

Se recomienda el cambio de las contraseñas como mínimo cada 3 meses y no deben ser reutilizadas.

En caso de sospecha, perdida, o uso indebido de los mecanismos de autenticación se debe notificar por escrito de inmediato al Notario y al Comité de Seguridad de la Información.

## *11.6 CONTROL DE ACCESO Y MECANISMOS DE AUTENTICACIÓN.*

Las redes de datos, lugares de almacenamiento, y demás recursos de la notaría deben ser debidamente protegidas contra accesos no autorizados a través de mecanismos de autenticación, o control de acceso.

Se debe asegurar que las redes inalámbricas de la organización cuenten con métodos de autenticación que evite accesos no autorizados.

Se tienen que verificar periódicamente los controles de acceso, mecanismo de autenticación y privilegios de funcionarios y usuarios provistos por terceras partes, con el fin de revisar que dichos usuarios tengan únicamente el acceso permitido a aquellos recursos y servicios para los que fueron autorizados.

Es obligatorio contar con el formato de creación de mecanismos de autenticación debidamente autorizado y Acuerdo de Confidencialidad, firmado previamente.
Los equipos de cómputo de usuario final que se conecten o deseen conectar a las redes de datos de las dependencias del Notario, deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

Todas las redes con salida a redes públicas deben ser aseguradas con los mecanismos de seguridad pertinentes (Firewalls, mecanismos de autenticación y protocolos de comunicación seguros).

El Notario establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos físicos, tecnológicos y los sistemas de información.

Se velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y para que la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

# 12 DEL TRATAMIENTO Y ALMACENAMIENTO DE INFORMACIÓN SENSIBLE Y CONFIDENCIAL.

El Comité de Seguridad de la información debe garantizar y controlar el tratamiento de la información sensible y confidencial, por parte de los directivos, funcionarios y terceros, conforme lo exigen las normas legales vigentes.

Si la información sensible y confidencial es almacenada, se debe incluir con metadatos y funciones hash para garantizar la integridad y no repudio de la información y debe ser conforme la Política de Seguridad de la Información de la notaría y los estándares y disposiciones legales vigentes.

# 13 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

Todo el personal que tenga relación con los activos de la información del Notario está obligado a reportar, con responsabilidad, presuntas violaciones a la seguridad de la información de la notaría.

El Comité de Seguridad de la Información de la notaría es el encargado de preparar,

mantener y difundir los procesos y normas para el reporte de investigación de incidentes de seguridad de la información.

De acuerdo a la ley y a la Política de Seguridad de la Información de la notaría el Notario y/o el Comité de Seguridad de la Información están autorizados para realizar seguimiento o interceptación a los mecanismos o recursos que permitan determinar incidentes en la seguridad de la información.

# 14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS SOFTWARE.

El Comité de Seguridad de la información debe asegurar y controlar que el hardware o software, adquirido por el Notario, y sus correspondientes mantenimientos se realicen respetando la Política de Seguridad de la Información de la notaría.

El Comité de Seguridad de la Información de la notaría debe asegurar y controlar el procesamiento correcto de las aplicaciones adquiridas por el Notario para evitar errores, pérdida, modificaciones no-autorizadas o mal uso de la información en las aplicaciones.

El Comité de Seguridad de la Información de la notaría debe chequear y validar las aplicaciones adquiridas, para evitar y controlar los errores de procesamiento o mal uso de estas. También debe identificar los requerimientos de dichas aplicaciones para asegurar, controlar y proteger la autenticidad, integridad y disponibilidad del mensaje

- Los procesos operativos y estratégicos de la notaría son apoyados con el uso de las

  tecnologías de la información y las comunicaciones.

- El software utilizado por la notaría es adquirido a terceros, que son quienes desarrollan las soluciones, las implementan y realizan el mantenimiento preventivo y correctivo.

- El Notario es el encargado de elegir, autorizar y comprar el hardware y las aplicaciones informáticas a utilizar en la Notaría.

- El Notario debe evitar autorizar la implementación de software que tenga asociado riesgo alto no mitigado.

- El Notario debe asegurar que los aplicativos o sistemas informáticos, implementados en sus despachos, incluyen controles de seguridad y cumplen con la Política de Seguridad de la Información.

- El hardware o software adquirido debe especificar los requerimientos de los controles de seguridad.

- El Comité de Seguridad de la Información de la Notaría es el encargado de difundir procesos, lineamientos, estrategias, buenas prácticas, identificando los riesgos y la forma de mitigarlos, para asegurar la calidad en la implementación de la solución.

- El Comité de Seguridad de la Información es la única autorizada para realizar copia de seguridad del software original, siempre que esté estipulado en la licencia, para ser utilizada en caso de que el medio presente algún daño.

- El software adquirido por el Notario no puede ser copiado o suministrado a terceros.

- Está prohibido el uso e instalación de juegos en los computadores de la notaría.

# 15 CUMPLIMIENTO.

La Política de la Seguridad de la Información del Notario y los estándares de seguridad de las informaciones legales vigentes son de obligatorio cumplimiento por directores, funcionarios, usuarios y terceros. Este cumplimiento se debe tener como condición al momento de realizar contrataciones, compromisos o acuerdos con personal que tenga relación con los activos de la información del Notario.

La Política de la Seguridad de la Información de la notaría se empieza a implementar con la aprobación del texto de este documento y el plazo máximo para la implementación total de la Política de Seguridad de la Información en la notaría es de 2 meses.